On the Weight Distribution of Codes over Finite Rings

Eimear Byrne

School of Mathematical Sciences, University College Dublin

Abstract

Let $R > S$ be finite Frobenius rings for which there exists a trace map $T : {}_S R \longrightarrow {}_S R$. Let $C_{f,S} := \{x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R\}$. $C_{f,S}$ is an S-linear subring-subcode of a left linear code over R. We consider functions f for which the homogeneous weight distribution of $C_{f,S}$ can be computed. In particular, we give constructions of codes over integer modular rings and commutative local Frobenius that have small spectra.

Key words: ring-linear code, homogeneous weight, weight distribution, character module

1 Introduction

The homogeneous weight, introduced for integer residue rings in [8] and extended for arbitrary finite rings in [10], has been studied extensively in the context of ring-linear coding. It can be viewed as a generalization of the Hamming weight; in fact it coincides with the Hamming weight when the underlying ring is a finite field and is the Lee weight when defined over $\mathbb{Z}_4$. Many of the classical results for codes over finite fields for the Hamming weight have corresponding homogeneous weight versions for codes over finite rings. The MacWilliams equivalence theorem holds for codes over finite Frobenius rings and quasi-Frobenius modules with respect to the homogeneous weight [10,11]. Analogues of several classical bounds have been found for this weight function

Email address: ebyrne@ucd.ie (Eimear Byrne).

[1] Research supported by the Science Foundation of Ireland, 08/RFP/MTH1181

[3,4,12]. Combinatorial objects such as strongly regular graphs can be constructed from codes over finite Frobenius rings with exactly two nonzero homogeneous weights [2,5,16]. Although homogeneous weights exist on any finite ring, if the ring in question is Frobenius, these weight functions can be expressed in terms of a character sum [15], a property we shall use here.

Let $\mathrm{Tr} : \mathrm{GF}(q^r) \longrightarrow GF(q)$ be the usual trace map from $GF(q^r)$ onto $GF(q)$. Let $f : \mathrm{GF}(q^r) \longrightarrow GF(q^r)$ be an arbitrary map. A construction of a $GF(q)$-linear subspace-subcode is given by:

$$C_f := \{c^f_{\alpha,\beta} : \mathrm{GF}(q^r) \longrightarrow GF(q) : x \mapsto \mathrm{Tr}(\alpha x + \beta f(x)), \alpha, \beta \in GF(q^r)\}.$$

This has arisen in the literature on perfect and almost perfect nonlinear functions (c.f. [1,6,20]) and on cyclic codes (in which case f is a power map). In the case of an APN function on a field of even characteristic it is sometimes possible to determine the distinct weights or the weight distribution of the resulting code, or equivalently the Walsh spectrum of f. In [7], perfect nonlinear maps were used to construct (in some cases optimal) codes for use in secret sharing schemes.

Here we consider the same code construction for codes over finite rings, specifically, some integer modular rings, Galois rings and local commutative Frobenius rings.

2 Preliminaries

We recall some properties of finite rings that meet our purposes. Further details can be read in [15,17,18,19]. For a finite ring R, we denote by $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$, the group of additive characters of R. $\hat{R}$ is an R-R bi-module according to the relations

$$^r\chi(x) = \chi(rx), \quad \chi^r(x) = \chi(xr),$$

for all $x, r \in R, \chi \in \hat{R}$. A character χ is called left (resp. right) generating if given any $\phi \in \hat{R}$ there is some $r \in R$ satisfying $\phi = {}^r\chi$ (resp. $\phi = \chi^r$). The next result gives a characterization of finite Frobenius rings.

Theorem 2.1 *Let R be a finite ring. The following are equivalent.*

(1) R is a Frobenius ring
(2) $\mathrm{Soc}\,_RR$ is left principal,
(3) $_R(R/Rad\ R) \simeq \mathrm{Soc}\,_RR$,
(4) $_RR \simeq {}_R\hat{R}$

Then ${}_R\hat{R} = {}_R\langle\chi\rangle$ for some (left) generating character χ. It can be shown that any left generating character is also a right generating character.

Integer residue rings, finite chain rings, semi-simple rings, principal ideal rings, direct products of Frobenius rings, matrix rings over Frobenius rings, group rings over Frobenius rings are all examples of Frobenius rings. The results of this paper are restricted to the case where the code's alphabet is an integer modular ring or a local commutative Frobenius ring.

Let R be a finite commutative local Frobenius ring with unique maximal ideal M and residue field $K = R/M$ of order q for some prime power q. Then $M = \operatorname{Rad} R$ and $\operatorname{Soc} R = R/M$ is simple. Moreover, $\operatorname{Soc} R$ is the annihilator of $\operatorname{Rad} R$, which we write as $\operatorname{Soc} R = M^{\perp}$. $R^{\times}$ contains a unique cyclic subgroup G of order $|K^{\times}|$. We call $\mathcal{T} := G \cup \{0\}$ the *Teichmuller set* of R. Later, we will use that fact that each element $a \in R$ can be expressed uniquely as $a = a_t + a_m$ for some unique $a_t \in \mathcal{T}$, $a_m \in M$. We define the map $\nu : R \longrightarrow \mathcal{T} : a \mapsto a_t$.

If the local commutative ring R is the Galois ring $GR(p^n, r)$, of order p^{nr} and characteristic p^n, then each element $a \in R$ can be expressed uniquely in the form $a = a_0 + pa_1 + \cdots + p^{n-1}a_{n-1}$ for some unique $a_i \in \mathcal{T}$.

For an arbitrary finite ring, the homogeneous weight is defined as follows [8,10].

Definition 2.2 *Let R be a finite ring. A weight $w : R \longrightarrow \mathbb{Q}$ is* (left) homogeneous*, if $w(0) = 0$ and*

(1) If $Rx = Ry$ then $w(x) = w(y)$ for all $x, y \in R$.
(2) There exists a real number γ such that

$$\sum_{y \in Rx} w(y) \;=\; \gamma\,|Rx| \qquad \textit{for all } x \in R \setminus \{0\}.$$

Example 1 *On every finite field $\mathbb{F}_q$ the Hamming weight is a homogeneous weight of average value $\gamma = \frac{q-1}{q}$.*

Example 2 *On the ring $\mathbb{Z}_{pq}, p, q$ prime, a homogeneous weight with average value*

$\gamma = 1$ *is given by*

$$w : R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ \frac{p}{p-1} & \text{if } x \in p\mathbb{Z}_{pq}, \\ \frac{q}{q-1} & \text{if } x \in q\mathbb{Z}_{pq}, \\ \frac{pq-p-q}{pq-p-q+1} & \text{otherwise.} \end{cases}$$

Example 3 *On a local Frobenius ring R with q-element residue field the weight*

$$w : R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ \frac{q}{q-1} & \text{if } x \in \mathrm{Soc}(R),\ x \neq 0, \\ 1 & \text{if otherwise,} \end{cases}$$

is a homogeneous weight of average value $\gamma = 1$.

A description of the homogeneous weight in terms of sums of generating characters is given by the following [15].

Theorem 2.3 *Let R be a finite Frobenius ring with generating character χ. Then the homogeneous weights on R are precisely the functions*

$$w : R \longrightarrow \mathbb{R}, \quad x \mapsto \gamma \Big[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \Big]$$

where γ is a real number.

Unless otherwise stated, we will set $\gamma = 1$ (the *normalized* homogeneous weight).

3 Characters and Trace Maps

Definition 3.1 *Let $R > S$ be Frobenius rings. An S-module epimorphism $T : {}_SR \longrightarrow {}_SS$ whose kernel contains no non-trivial left ideal of R is called a trace map from R onto S.*

Example 4 *Recall that a finite Frobenius ring R has a generating character χ. Let R have characteristic m. Then we can implicitly define a trace map T from R onto its characteristic subring $\mathbb{Z}_m$ by $\chi(x) = \omega^{T(x)}$ for all x, where ω is a primitive complex mth root of unity. This is the absolute trace map on R.*

Given a trace map $T : {}_S R \longrightarrow {}_S S$, a generating character $\Phi \in \hat{S}$ determines a generating character $\chi \in \hat{R}$ by:

$$\chi(x) = \Phi(T(x)) \; \forall \; x \in R.$$

Example 5 *Let S be a finite Frobenius ring and let $R = M_n(S)$. Then R is Frobenius and the usual trace map*

$$\mathrm{tr} \; : R \longrightarrow S : (a_{ij}) \mapsto \sum_{i=1}^{n} a_{ii}$$

is an epimorphism onto S whose kernel contains no non-trivial left ideal of R. A generating character $\Phi \in \hat{S}$ induces a generating character $\chi = \mathrm{tr} \circ \Phi \in \hat{R}$.

Example 6 *Let $R = GR(p^n, sk), S := GR(p^n, s)$ be Galois rings of characteristic p^n and orders p^{nsk}, p^{ns}, respectively. As in the case of a finite field, R has a cyclic automorphism group of order sk [19]. Each element $a \in R$ has a canonical representation in the form $a = \sum_{i=0}^{n} p^i a_i$ for some unique a_i in the Teichmuller set of R. With respect to this expression,*

$$\sigma : R \longrightarrow R : \sum_{i=0}^{n} p^i a_i \mapsto \sum_{i=0}^{n} p^i a_i^p$$

generates $Aut(R)$, and $\tau := \sigma^s$ generates $Aut(R : S)$, the group of S-automorphisms of R. The map

$$T_{R/S} : R \longrightarrow S : a \mapsto a + \tau(a) + \cdots + \tau^{(k-1)}(a)$$

is a trace map from R onto S. Observe that as in the field case, $T_{R/S}(\tau(a)) = T_{R/S}(a)$ for any $a \in R$.

Example 7 *Let $R = \mathbb{Z}_4[x]/\langle x^2 + 2 \rangle$. Then every element $r \in R$ can be expressed uniquely in the form $r = r_0 + \theta r_1$, where $\theta^2 = 2 \; r_i \in \mathbb{Z}_4$. A $\mathbb{Z}_4$-epimorphism from R onto $\mathbb{Z}_4$ must have the form $T_\lambda : R \longrightarrow \mathbb{Z}_4 : r_0 + \theta r_1 \mapsto \lambda_0 r_0 + \lambda_1 r_1$ for some $\lambda_i \in \mathbb{Z}_4$. This gives a trace map if and only if $\lambda_1 \in \mathbb{Z}_4^\times$, so there are exactly 8 distinct trace maps from R onto $\mathbb{Z}_4$. Each such map determines a generating character χ defined by $\chi^\lambda(x) = \omega^{T_\lambda(x)}$ for all $x \in R$. Note that $Aut(R)$ is cyclic of order 2 generated by $\sigma : r_0 + \theta r_1 \mapsto r_0 - \theta r_1$. It is easy to check that $T_\lambda \circ \sigma = T_{\sigma(\lambda)} \neq T_\lambda$ for $\lambda_1 \in \mathbb{Z}_4^\times$.*

4 Subring Subcodes

For the remainder, let $R > S$ be finite Frobenius rings and assume there is a trace map $T : {}_SR \longrightarrow {}_SS$. Let Φ be a generating character of S and let $\chi := \Phi \circ T$. For any map $f : R \longrightarrow R$, we define the left S-linear subring subcode

$$C_{f,S} := \{c^f_{\alpha,\beta} : R \longrightarrow S : x \mapsto T(\alpha x + \beta f(x)) : \alpha, \beta \in R\}.$$

For the case $R = S$, we write $C_f := C_{f,R}$. We extend the homogeneous weight on S to the module of functions from R to S by $w(g) := \sum_{x \in R} w(g(x))$ for an arbitrary map $g : R \longrightarrow S$. We thus compute the weight of each codeword as:

$$\begin{aligned} w(c^f_{\alpha,\beta}) &= \sum_{x \in R} w(c^f_{\alpha,\beta}(x)) \\ &= |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \Phi^u(T(\alpha x + \beta f(x))) \\ &= |R| - \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)). \end{aligned}$$

Definition 4.1 *Let $f : R \longrightarrow R$. For each $\alpha, \beta \in R$, we define the transform*

$$W^{f,S}(\alpha, \beta) := \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x + \beta f(x)) = |R| - w(c^f_{\alpha,\beta}).$$

The spectrum of f is defined to be the set

$$\Lambda_{f,S} := \{W^{f,S}(\alpha, \beta) : \alpha, \beta \in R\}.$$

In keeping with the above, we write $W^f := W^{f,R}$ and $\Lambda_f := \Lambda_{f,R}$.

Observe that if $|\Lambda_{f,S}| = k + 1$ then $C_{f,S}$ has exactly k non-zero weights. Clearly,

$$W^{f,S}(\alpha, 0) = \begin{cases} \frac{1}{|S^\times|} \sum_{u \in S^\times} \sum_{x \in R} \chi^u(\alpha x) = |R| & \text{if } \alpha = 0 \\ 0 & \text{if } \alpha \neq 0. \end{cases}$$

In particular, if f is R-linear then $C_{f,S}$ is a one-weight code with constant non-zero weight $|R|$.

For a code C with distinct homogeneous weights $W \subset \mathbb{Q}$ we define the (homogeneous) weight enumerator of C by $\sum_{w \in W} A_w X^w$, where $A_w = |\{c \in C : w(c) = w\}|$[2].

5 Families of Codes with Few Weights

We now present some families of codes whose weight distributions can be computed.

5.1 Galois Rings

The class of functions discussed in the next theorem is a variant of the family of Frank sequences (c.f. [14]) . Such sequences and their generalizations form a family of perfect sequences, having the property that their Fourier transforms have constant absolute value.

Theorem 5.1 *$R = GR(p^2, r), S = GR(p^2, s), p$ prime, for some positive integers r, s, k satisfying $sk = r$ and $k > 1$. Let $\mathcal{T}$ denote the Teichmuller set of R, let $q = p^s$ and let π be a permutation of $\mathcal{T}$ that fixes 0. Write $x = x_0 + px_1$, $x_i \in \mathcal{T}$ for each $x \in R$. Let*

$$f : R \longrightarrow R : x \mapsto p\pi(x_0)x_1.$$

Then

$$\Lambda_{f,S} = \{q^{2k}, q^k, -\frac{q^k}{q-1}, 0\}.$$

Proof: Let $\alpha, \beta \in R$. Then $\alpha x + \beta f(x) = \alpha x_0 + p(\alpha + \beta\pi(x_0))x_1$, and so

[2] Note that as defined, this weight enumerator is not necessarily a polynomial, although this could be achieved by choosing appropriate γ, for example, $\gamma = |R^\times|$.

$$\begin{aligned}
W^{f,S}(\alpha,\beta) &= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{x\in R}\chi^u(\alpha x+\beta f(x))\\
&= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{x\in R}\chi^u(\alpha x_0+p(\alpha+\beta\pi(x_0))x_1)\\
&= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{x_0\in\mathcal{T}}\chi^u(\alpha x_0)\sum_{x_1\in\mathcal{T}}\chi^u(p(\alpha+\beta\pi(x_0))x_1)\\
&= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{T}}\chi^u(\alpha t)\sum_{z\in pR}\chi^u((\alpha+\beta\pi(t))z)\\
&= \frac{|pR|}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{V}}\chi^u(\alpha t),
\end{aligned}$$

where $\mathcal{V}=\{t\in\mathcal{T}:\alpha+\beta\pi(t)\in pR\}$.

For the case $\beta\in pR$, we have $W^{f,S}(\alpha,\beta)=W^{f,S}(\alpha,0)$, which takes the value zero if $\alpha\neq 0$ and $|R|$ otherwise. For arbitrary $\alpha,\beta\in R$ we have

$$\begin{aligned}
W^{f,S}(\alpha,\beta) &= \frac{|pR|}{|S^\times|}\sum_{t\in\mathcal{V}}\left(\sum_{u\in S}\chi(\alpha tu)-\sum_{u\in pS}\chi(\alpha tu)\right)\\
&= \frac{|pR|}{|S^\times|}\sum_{t\in\mathcal{V}}\left(\sum_{u\in S}\Phi(T_{R/S}(\alpha t)u)-\sum_{u\in pS}\Phi(T_{R/S}(\alpha t)u)\right)\\
&= \frac{|pR|}{|S^\times|}(|S||\mathcal{V}\cap U_0|-|pS||\mathcal{V}\cap U_1|),
\end{aligned}$$

where $U_0=\{t\in\mathcal{T}:T_{R/S}(\alpha t)=0\}$ and $U_1=\{t\in\mathcal{T}:T_{R/S}(\alpha t)\in pR\}$.

For the case $\beta\in R^\times$, $\mathcal{V}=\{\pi^{-1}(\nu(-\alpha\beta^{-1}))\}$. If $\alpha\in pR$ then $W\cap U_0=W\cap U_1=W=\{0\}$ and so $W^{f,S}(\alpha,\beta)=|pR|$. If $\alpha\in R^\times$, then

$$W^{f,S}(\alpha,\beta)=\begin{cases}\frac{|pR|}{|S^\times|}(|S|-|pS|)=|pR|=q^k & \text{if } T_{R/S}(\alpha\pi^{-1}(\nu(-\alpha\beta^{-1})))=0,\\ \frac{|pR|}{|S^\times|}(-|pS|)=-\frac{q^k}{q-1} & \text{if } T_{R/S}(\alpha\pi^{-1}(\nu(-\alpha\beta^{-1})))\in pS\backslash\{0\},\\ 0 & \text{otherwise.}\end{cases}$$

The result follows. □

Corollary 8 *Let $C_{f,S}$ be defined as in Theorem 5.1. Then $C_{f,S}$ has size q^{3k}, and weight enumerator*

$$1+(q^k-1)\left((q^{2k-2}-q^{k-1}+q^k)X^{q^{2k}-q^k}+(q^{2k}-q^{2k-1}+q^k+1)X^{q^{2k}}\right.$$
$$\left.+(q^{2k-1}-q^k-q^{2k-2}+q^{k-1})X^{q^{2k}+\frac{q^k}{q-1}}\right).$$

Proof: Since $\ker T_{R/S}$ contains no non-trivial ideal, $T_{R/S}(\alpha x+p\beta\pi(x_0)x_1)=0$ for all $x\in R$ if and only if $\alpha=0$ and $\beta\in pR$. It follows that $|C_f|=q^{3k}$. Moreover, given any $\alpha,\alpha',\beta,\beta'\in R$, $c^f_{\alpha,\beta}=c^f_{\alpha',\beta'}$ if and only if $\alpha=\alpha'$ and $\beta-\beta'\in pR$. For $\beta\in R^\times$, the map $\alpha\mapsto\alpha\pi^{-1}(\nu(-\alpha\beta^{-1}))$ is a permutation on $R^\times$. Then $|\{\alpha\in R^\times : T_{R/S}(\alpha\nu(\pi(-\alpha\beta^{-1})))=\theta\}|=|\{\alpha\in R^\times : T_{R/S}(\alpha)=\theta\}|$ for any $\theta\in R$. Now $|\ker T_{R/S}\cap R^\times|=|\ker T_{R/S}|-|\ker T_{R/S}\cap pR|=q^{2(k-1)}-q^{k-1}$ and $|(\ker T_{R/S}+pR)\cap R^\times|=|\ker T_{R/S}+pR|-|(\ker T_{R/S}+pR)\cap pR|=q^{2k-1}-q^k$. We summarize these observations along with results of Theorem 5.1 in the table shown below, from which the statement of the theorem follows.

$w(c^f_{\alpha,\beta})$	constraints on α,β	$\lvert\{c^f_{\alpha,\beta}\}\rvert$
0	$\beta=0,\ \alpha=0.$	1
$q^{2k}-q^k$	$\beta\in\mathcal{T}\backslash\{0\},\alpha\in pR;$ $\beta\in\mathcal{T}\backslash\{0\},\alpha\in R^\times$ and $T_{R/S}(\alpha\nu(-\alpha\beta^{-1}))=0.$	$(q^k-1)q^k+(q^k-1)(q^{2(k-1)}-q^{k-1})$
q^{2k}	$\beta=0,\alpha\neq0;$ $\beta\in\mathcal{T}\backslash\{0\},\alpha\in R^\times$ and $T_{R/S}(\alpha\nu(-\alpha\beta^{-1}))\notin pS.$	$q^{2k}-1+(q^k-1)(q^{2k}-q^{2k-1})$
$q^{2k}+\dfrac{q^k}{q-1}$	$\beta\in\mathcal{T}\backslash\{0\},\alpha\in R^\times$ and $T_{R/S}(\alpha\nu(-\alpha\beta^{-1}))\in pS\backslash\{0\}.$	$(q^k-1)q^{k-1}(q^{k-1}-1)(q-1)$

□

For the case $R=S$, the code corresponding to $f: x\mapsto p\pi(x_0)x_1$ is a two-weight code.

Corollary 9 *Let f be defined as in Theorem 5.1. Then*

$$\Lambda_f=\{p^{2r},p^r,0\},$$

and C_f has weight enumerator

$$1+(p^{2r}-p^r)X^{p^{2r}-p^r}+(p^{3r}-p^{2r}+p^r-1)X^{p^{2r}}.$$

Proof: Let $\alpha, \beta \in R$. Almost exactly as in the proof of Theorem 5.1 we have

$$W^f(\alpha,\beta) = \frac{|pR|}{|R^\times|}(|R||\mathcal{V} \cap U_0| - |pR||\mathcal{V} \cap U_1|),$$

where $U_0 = \{t \in \mathcal{T} : \alpha t = 0\}$ and $U_1 = \{t \in \mathcal{T} : \alpha t \in pR\}$. If $\alpha \in R^\times$ then $W \cap U_0 = W \cap U_1 = \emptyset$. □

5.2 Integer Modular Rings

Cyclic codes on finite fields have been well studied. It is surely well known and not hard to show the following.

Theorem 5.2 *Let $R = \mathbb{Z}_p$, p prime, let $d \in \{2, ..., p-1\}$ then C_{x^d} is a two-weight code with Hamming weight enumerator*

$$1 + \frac{(p-1)^2}{\ell} X^{p-\ell-1} + \left(p^2 - 1 - \frac{(p-1)^2}{\ell}\right) X^{p-1},$$

where $(d-1, p-1) = \ell$.

We compute the weight distribution of a family of cyclic codes C_{x^d} on $\mathbb{Z}_{2p}$, which turn out to be two-weight codes.

Theorem 5.3 *Let $R = \mathbb{Z}_{2p}, p$ prime. Let $d \in \{2, ..., p-1\}$, let $\ell = (d-1, p-1)$ and let $f : R \longrightarrow R : x \mapsto x^d$. Then*

$$\Lambda_f = \{2p, \frac{2p\ell}{p-1}, 0\}.$$

and C_{x^d} has weight enumerator

$$1 + \frac{(p-1)^2}{\ell} X^{2p\frac{p-1-\ell}{p-1}} + \left(2p^2 - \frac{(p-1)^2}{\ell} - 1\right) X^{2p}.$$

Proof: The map $x \mapsto \alpha x + \beta x^d$ is identically zero if and only if $\alpha = \beta \in pR$. In particular, $|C_f| = 2p^2$ and $c^f_{\alpha,\beta} = c^f_{\alpha',\beta'}$ if and only if $\alpha = \alpha' + p, \beta = \beta' + p$. We compute

$$
\begin{aligned}
W^f(\alpha,\beta) &= \frac{1}{p-1}\sum_{x\in R}\Bigg(\sum_{u\in R}\chi(u(\alpha x+\beta x^d)) - \sum_{u\in pR}\chi(u(\alpha x+\beta x^d)) \\
&\quad - \sum_{u\in 2R}\chi(u(\alpha x+\beta x^d)) + 1\Bigg) \\
&= \frac{1}{p-1}(2p|X| - 2|X_2| - p|X_p| + 2p),
\end{aligned}
$$

where $X = \{x \in R : \alpha x + \beta x^d = 0\}$, $X_2 = \{x \in R : \alpha x + \beta x^d \in 2R\}$ and $X_p = \{x \in R : \alpha x + \beta x^d \in pR\}$. For each $\gamma \in R^\times$, the map $\alpha \mapsto (-\alpha\gamma^{-1})^{\frac{\ell}{d-1}}$ is a permutation of $2R\backslash\{0\}$ if $\alpha \in 2R\backslash\{0\}$ and of $R^\times$ if $\alpha \in R^\times$. Moreover, for each divisor ℓ of $p-1$, there are $\frac{p-1}{\ell}$ distinct ℓth roots of unity in $R^\times$ and hence $\frac{(p-1)^2}{\ell}$ pairs α, γ such that $(-\alpha\gamma^{-1})^{\frac{\ell}{d-1}}$ has an ℓth root in $R^\times$ if $\alpha \in R^\times$ (resp. $2R$ if $\alpha \in \backslash\{0\}$) . The results are summarized below.

$\lvert X\rvert$	$\lvert X_2\rvert$	$\lvert X_p\rvert$	$W^f(\alpha,\beta)$	α,β
$2(\ell+1)$	$2p$	$2(\ell+1)$	$\dfrac{2p\ell}{p-1}$	$\alpha = 2\alpha_1, \beta = 2\beta_1 \in 2R\backslash\{0\}$, $-\alpha_1\beta_1^{-1}$ has a υth root in R
2	$2p$	2	0	$\alpha = 2\alpha_1, \beta = 2\beta_1 \in 2R\backslash\{0\}$, $-\alpha_1\beta_1^{-1}$ has no υth root in R
$\ell+1$	p	$2(\ell+1)$	0	$\alpha = 2\alpha_1 \in 2R\backslash\{0\}$, $\beta \in R^\times -2\alpha_1\beta^{-1}$ has a υth root in $2R$
1	p	2	0	$\alpha = 2\alpha_1 \in 2R\backslash\{0\}, \beta \in R^\times$, $-2\alpha_1\beta^{-1}$ has no υth root in $2R$
2	$2p$	2	0	$\alpha = 0, \beta \in 2R\backslash\{0\}$
1	p	2	0	$\alpha = 0, \beta \in R^\times$
2	$2p$	2	0	$\alpha \in 2R\backslash\{0\}, \beta = 0$
2	$2p$	2	0	$\alpha \in R^\times, \beta = p$
p	p	$2p$	0	$\alpha = p, \beta = 0$
$2p$	p	2	$2p$	$\alpha = \beta = 0$

□

Given a two-weight code C with non-zero weights $w_1 < w_2$, we form the graph $G(C) = (V, E)$ by setting $V = C$ and $(x, y) \in E$ if and only if $w(x - y) = w_1$. A linear code C, with alphabet a finite Frobenius ring R and generated by the $k \times n$ matrix $Y = (y_1, ..., y_n)$ over R is called *modular* if there is some $r \in \mathbb{Q}$ such that $|\{i : y_i R = y_j R\}| = r|y_j R^\times|$ for each j.

Theorem 5.4 (Honold [16]) *Let C be a modular linear code defined over a finite Frobenius ring with exactly two distinct non-zero weights. Then $G(C)$ is a strongly regular graph.*

In fact for the finite field case, Theorem 5.4 is easily deduced from [9, Th. 2]. We now show that the code C_{x^d} on $\mathbb{Z}_p$ determines a strongly regular graph.

Corollary 10 *Let $R = \mathbb{Z}_p$, p prime, let $d \in \{2, ..., p-1\}$ and let $\ell = (d-1, p-1)$. Then C_{x^d} determines a strongly regular graph.*

Proof: To establish the modular property we must show that $|\{y \in \mathbb{Z}_p^\times : c^{x^d}_{\alpha,\beta}(y) = \lambda c^{x^d}_{\alpha,\beta}(x)\ \forall \alpha, \beta \in \mathbb{Z}_p\}| = r(p-1)$, independently of our choice of x for some $r \in \mathbb{Q}$. Let $x \in \mathbb{Z}_p^\times$. Then

$$\lambda c^{x^d}_{\alpha,\beta}(x) = \alpha(\lambda x) + \beta\lambda^{p-d}(\lambda x)^d = c^{x^d}_{\alpha,\beta\lambda^{p-d}}(\lambda x) = c^{x^d}_{\alpha,\beta}(\lambda x),$$

for all $\alpha, \beta \in \mathbb{Z}_p$ if and only if $\lambda^{d-1} = 1$. Then

$$|\{y \in \mathbb{Z}_p^\times : c^{x^d}_{\alpha,\beta}(y) = \lambda c^{x^d}_{\alpha,\beta}(x)\ \forall \alpha, \beta \in \mathbb{Z}_p\}| = |\{\lambda x : \lambda^{d-1} = 1\}| = \ell.$$

Thus C_{x^d} is a modular two-weight code. The parameters $[n, k, \lambda, \mu]$ are uniquely determined by the parameters of C_{x^d} (c.f. [2,16]) □

Remark 1 *The codewords of C_{x^d} defined over $\mathbb{Z}_p$ form an orthogonal array $OA(p, p-1)$ whenever $(d-1, p-1) = 1$. It is not hard to see that for $(d-1, p-1) = \ell > 1$, the graph $G(C)$ is isomorphic to one induced by an orthogonal array $OA(p, \frac{p-1}{\ell})$.*

Remark 2 *The codes $C_{p\pi(x_0)x_1,\mathbb{Z}_{p^2}}$ and the codes C_{x^d}, defined on $\mathbb{Z}_{2p}$, are never modular, so that Theorem 5.4 does not apply even though they are two-weight codes. Indeed in general the resulting graphs $G(C_{p\pi(x_0)x_1,\mathbb{Z}_{p^2}})$ and $G(C_{x^d})$ are disconnected.*

5.3 Local Commutative Rings

For this construction, we assume the existence of $\sigma \in Aut(R)$ such that $\chi \circ \sigma = \chi$ on R. For R a finite field, the function described in the next lemma is the map : $x \mapsto x^{p^k+1}$, which is known to be perfect nonlinear on a field of odd characteristic, and almost perfect nonlinear on a field of even characteristic.

Lemma 5.5 *Let $\sigma \in Aut(R)$ satisfy $\chi(\sigma(x)) = \chi(x)$ for all $x \in R$. Define*

$$f : R \longrightarrow R : a \mapsto \sigma(a)a - \sigma(a_m)a_m.$$

Then

$$W^{f,S}(\alpha,\beta) = \frac{|M|}{|S^\times|}\left(|S||\mathcal{V}\cap U_0| - |S\cap M||\mathcal{V}\cap U_1|\right),$$

where $\mathcal{V} = \{t \in \mathcal{T} : \alpha + \beta\sigma(t) + \sigma^{-1}(\beta t) \in \operatorname{Soc} R\}$, $U_0 = \{t \in \mathcal{T} : T(\alpha t + \beta\sigma(t)t) = 0\}$ and $U_1 = \{t \in \mathcal{T} : T(\alpha t + \beta\sigma(t)t) \in \operatorname{Soc} S\}$.

Proof: Let $\alpha, \beta \in R$

$$\begin{aligned} W^{f,S}(\alpha,\beta) &= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{x\in R}\chi^u(\alpha x + \beta(\sigma(x)x - \sigma(x_m)x_m)),\\ &= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{T}}\sum_{m\in M}\chi^u(\alpha(t+m) + \beta(\sigma(t+m)(t+m) - \sigma(m)m)),\\ &= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{T}}\chi^u(\alpha t + \beta\sigma(t)t)\sum_{m\in M}\chi^u(\alpha m + \beta(\sigma(t)m + \sigma(m)t)),\\ &= \frac{1}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{T}}\chi^u(\alpha t + \beta\sigma(t)t)\sum_{m\in M}\chi^u((\alpha + \beta\sigma(t) + \sigma^{-1}(\beta t))m), \end{aligned}$$

since $\chi(\sigma(x)) = \chi(x)$ for all $x \in R$. The character $\chi^u((\alpha+\beta\sigma(t)+\sigma^{-1}(\beta t))\cdot)$ is trivial on M if and only if $\alpha + \beta\sigma(t) + \sigma^{-1}(\beta t)$ annihilates every element of M. Therefore

$$W^{f,S}(\alpha,\beta) = \frac{|M|}{|S^\times|}\sum_{u\in S^\times}\sum_{t\in\mathcal{V}}\chi^u(\alpha t + \beta\sigma(t)t),$$

where $\mathcal{V} = \{t \in \mathcal{T} : \alpha + \beta\sigma(t) + \sigma^{-1}(\beta t) \in \operatorname{Soc} R\}$. Since S is local, we have $S^\times = S\backslash S\cap M$ and the annihilator ideal of $S \cap M$ in S is $\operatorname{Soc} S$, from which we deduce

$$\begin{aligned} W^{f,S}(\alpha,\beta) &= \frac{|M|}{|S^\times|}\sum_{t\in\mathcal{V}}\left(\sum_{u\in S}\Phi(uT(\alpha t + \beta\sigma(t)t)) - \sum_{u\in S\cap M}\Phi(uT(\alpha t + \beta\sigma(t)t))\right)\\ &= \frac{|M|}{|S^\times|}\left(|S||\mathcal{V}\cap U_0| - |S\cap M||\mathcal{V}\cap U_1|\right), \end{aligned}$$

where $U_0 = \{t \in \mathcal{T} : T(\alpha t + \beta\sigma(t)t) = 0\}$ and $U_1 = \{t \in \mathcal{T} : T(\alpha t + \beta\sigma(t)t) \in \operatorname{Soc} S\}$.

Example 11 *Let $R = \mathbb{Z}_2[x,y]/\langle x^2, y^2\rangle = \{a_1 + a_x x + a_y y + a_{xy}xy : a_X \in \mathbb{Z}_2\}$. R is a finite local Frobenius ring with Teichmuller set $\mathbb{Z}_2$ and maximal ideal $\langle x, y\rangle$. Each $a \in R$ has a unique expression in the form $a = a_t + a_m$ with $a_t = a_1 \in \mathbb{Z}_2$ and $a_m = a_y x + a_x y + a_{xy}xy$. The automorphism group of R has order 2 and is generated by*

$$\sigma : R \longrightarrow R : a_1 + a_x x + a_y y + a_{xy}xy \mapsto a_1 + a_y x + a_x y + a_{xy}xy.$$

It can be checked that the map

$$T : R \longrightarrow \mathbb{Z}_2 : a_1 + a_x x + a_y y + a_{xy}xy \mapsto a_1 + a_x + a_y + a_{xy}$$

is a trace map from R onto $\mathbb{Z}_2$ that induces the character $\chi : R \longrightarrow \mathbb{C}^\times$ defined by $\chi(a) = (-1)^{T(a)}$. Moreover, as $T \circ \sigma = T$, $\chi(\sigma(a)) = \chi(a)$ for all $a \in R$. If $f : R \longrightarrow R$ is defined as in Lemma 5.5 then $f(a) = a_1(1 + (a_x + a_y)(x + y))$ for each $a \in R$. With the same notation as in the lemma, for any $\alpha, \beta \in \mathbb{R}$, we have $U_0 = \{t \in \mathbb{Z}_2 : tT(\alpha + \beta) = 0\}$ and $U_1 = \mathbb{Z}_2$ so that $W^{f,\mathbb{Z}_2}(\alpha, \beta) = 8(2|\mathcal{V} \cap U_0| - |\mathcal{V}|)$, where $\mathcal{V} = \{t \in \mathbb{Z}_2 : \alpha + (\beta + \sigma(\beta))t \in \langle xy\rangle\}$. It is straightforward to check that $\Lambda_{f,\mathbb{Z}_2} = \{-8, 0, 8, 16\}$ and that $C_{f,\mathbb{Z}_2}$ is a three-weight code with Hamming weights $\{0, 4, 8, 12\}$ (setting $\gamma = \frac{q-1}{q}$ in the homogeneous weight). Its Hamming weight enumerator is given by $1 + 3X^4 + 27X^8 + X^{12}$.

Example 12 *Let R be the Galois ring $GR(2^3, 2)$ of characteristic 8 and order 64. As we saw in Example 6, Aut(R) is cyclic of order 2, generated by σ satisfying $T_{R/\mathbb{Z}_8} = T_{R/\mathbb{Z}_8} \circ \sigma$. Then with f defined as in Lemma 5.5, we have*

$$f(a_0 + 2a_1 + 4a_2) = 1 + 2(1 + a_0^2 a_1 + a_1^2 a_0) + 4(1 + a_0^2 a_2 + a_2^2 a_0).$$

We compute the distinct homogeneous weights of code $C_{f,\mathbb{Z}_8}$ as $\{0, 32, 48, 64, 80, 88, 96\}$.

Corollary 13 *Let $f : R \longrightarrow R$ be defined as in Lemma 5.5 Then*

$$\Lambda_{f,R} = \{|R|, |M|, \frac{|R||M|}{|R^\times|}, 0\}.$$

If $|K| > 2$ then $C_{f,R}$ has size $|R|^2$ and weight distribution

weight	*number of codewords*
0	1
$\lvert R\rvert - \lvert M\rvert$	$\lvert K\rvert\lvert R\rvert - \lvert K\rvert^2 + \lvert K\rvert - 1$
$\lvert R\rvert - \frac{\lvert R\rvert\lvert M\rvert}{\lvert R^\times\rvert}$	$\lvert K\rvert^2 - 2\lvert K\rvert + 1$
$\lvert R\rvert$	$\lvert R\rvert^2 - \lvert K\rvert\lvert R\rvert + \lvert K\rvert - 1$

.

If $|K| = 2$ *then* $|C_{f,R}| = \dfrac{|R|^2}{2}$ *and* $C_{f,R}$ *has weight enumerator*

$$1 + (|R| - 2)X^{\frac{|R|}{2}} + \left(\frac{|R|^2}{2} - |R| + 1\right) X^{|R|}.$$

Proof: We note that every element of $Aut(R)$ fixes $R^\times$, M and $\operatorname{Soc} R$. Let $\alpha, \beta \in R$. If $\alpha, \beta \notin \operatorname{Soc} R$ then $0 \notin \mathcal{V}$ and so

$$\mathcal{V} \cap U_1 = \{t \in \mathcal{T} \backslash \{0\} : \sigma^{-1}(\beta t) \in \operatorname{Soc} R\} = \emptyset = \mathcal{V} \cap U_0.$$

If $\alpha \in \operatorname{Soc} R, \beta \notin \operatorname{Soc} R$ then

$$\{0\} \subset \mathcal{V} \cap U_1 \subset \{t \in \mathcal{T} : \beta\sigma(t)t \in \operatorname{Soc} R\} = \{0\} = \mathcal{V} \cap U_0.$$

If $\alpha \notin \operatorname{Soc} R, \beta \in \operatorname{Soc} R$ then $\mathcal{V} = \emptyset$.

Suppose now that $\alpha, \beta \in \operatorname{Soc} R$. Then clearly $\mathcal{V} = U_1 = \mathcal{T}$. Since $\operatorname{Soc} R = M^\perp$ is principal in R, there exist unique $\alpha_u, \beta_u \in \mathcal{T}$ satisfying $\alpha = \alpha_u\theta$ and $\beta = \beta_u\theta$ for fixed θ generating $\operatorname{Soc} R$. Therefore,

$$U_0 = \{0\} \cup \{t \in \mathcal{T} \backslash \{0\} : \alpha_u + \beta_u\sigma(t) \in M\}.$$

If $\beta_u \neq 0$ then there is a unique $t \in \mathcal{T}$ satisfying $t \in \sigma^{-1}(-\alpha_u\beta_u^{-1}) + M$. If $\alpha_u = 0$ we have $|U_0| = 1$ and otherwise we have $|U_0| = 2$. If $\beta_u = 0$ then $U_0 = \{0\}$ unless $\alpha_u = 0$, in which case $U_0 = \mathcal{T}$. We summarize these observations in the table below.

$W^f(\alpha, \beta)$	α, β
$\lvert R\rvert$	$\alpha = \beta = 0$
$\lvert M\rvert$	$\alpha \in \operatorname{Soc} R, \beta \notin \operatorname{Soc} R$ or $\alpha \in \operatorname{Soc} R\backslash\{0\}, \beta = 0$
$\dfrac{\lvert R\rvert\lvert M\rvert}{\lvert R^\times\rvert}$	$\alpha, \beta \in \operatorname{Soc} R\backslash\{0\}$
0	$\alpha \notin \operatorname{Soc} R$ or $\alpha = 0, \beta \in \operatorname{Soc} R\backslash\{0\}$

.

Now $c^f_{\alpha,\beta}(x) = \alpha x + \beta(\sigma(x_t)x + \sigma(x_m)x_t)$. Suppose that $c^f_{\alpha,\beta}$ is identically zero. Then in particular, $c^f_{\alpha,\beta}(\theta) = \alpha\theta + \beta(\sigma(\theta)\theta = 0$ for any $\theta \in \mathcal{T}$, in which case $\alpha = -\beta\sigma(\theta)$ for any such nonzero θ. It follows that if $|K| = |\mathcal{T}| > 2$ then $\alpha = \beta = 0$. Therefore $|C_{f,R}| = |R|^2$, and $C_{f,R}$ has the weight distribution shown above. Suppose now that

$|K| = |\mathcal{T}| = 2$, so that $\mathcal{T} = \{0,1\}$, which is point-wise fixed by σ. Then $\alpha = -\beta$ and moreover, since $c^f_{\alpha,\beta}(m) = \alpha m$ for any $m \in M$, we must have $\alpha \in \operatorname{Soc} R$. Conversely, for any $\delta \in \operatorname{Soc} R$, $c^f_{\delta,-\delta}(x) = \delta(x(1-x_t) + \sigma(x_m)x_t)$ is the zero map. It follows that $|C| = \dfrac{|R|^2}{|\operatorname{Soc} R|} = \dfrac{|R|^2}{2}$ and that $C_{f,R}$ has the weight enumerator given above.

□

Example 14 *Let $R = \mathbb{Z}_2[x,y]/\langle x^2, y^2\rangle$ with f defined as in Example 11. Since $|K| = 2$, from Corollary 13 we deduce that C_f is a two-weight code over R of size 128 with homogeneous weight enumerator*

$$1 + 14X^8 + 113X^{16}.$$

Example 15 *Let $R = \mathbb{Z}_3[x,y]/\langle x^2, y^2\rangle$. Then R has residue field $K = GF(3)$, $|R| = 3^4, |M| = 3^3$ and $|R^\times| = 2.3^3$. Let $f(x) = \sigma(x)x - \sigma(x_m)x_m$ for $\sigma(a_1 + a_x x + a_y y + a_{xy}xy) = a_1 + a_y x + a_x y + a_{xy}xy$. Then from Corollary 13, C_f is a three-weight code over R of size $3^8 = 6561$ with weight enumerator*

$$1 + 4X^{\frac{81}{2}} + 236X^{54} + 6320X^{81}.$$

Example 16 *Let $R = \mathrm{GR}(2^3, 2)$, with f defined as in Example 12. Then C_f is a three-weight code over R of order 4096 with weight enumerator*

$$1 + 243X^{48} + 9X^{\frac{128}{3}} + 3843X^{64}.$$

Acknowledgement: The author is grateful to Marcus Greferath and Alexander Nechaev for useful discussions regarding trace maps on finite rings.

References

[1] C. Bracken, E. Byrne, N. Markin, G. McGuire *New Families of Almost Perfect Nonlinear Trinomials and Multinomials*, Finite Fields and Their Applications, 14 (3) (2008) 703–714.

[2] E. Byrne, M. Greferath and T. Honold, *Ring Geometries, Two-Weight Codes and Strongly Regular Graphs*, Designs, Codes and Cryptography, 48 (1) (2008) 1–16.

[3] E. Byrne, M. Greferath and M. E. O'Sullivan, *The Linear Programming Bound for Codes over Finite Frobenius Rings,* Designs, Codes and Cryptography, 42 , **3** (2007), 289–301.

[4] E. Byrne, M. Greferath, A. Kohnert, V. Skachek, *New Bounds for Codes Over Finite Frobenius Rings* Designs, Codes and Cryptography, 42 **3** (2010), Online First.

[5] E. Byrne, A. Sneyd, *Constructions of Two-Weight Codes Over Finite Rings*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010), Budapest, July, 2010.

[6] C. Carlet, P. Charpin, V. Zinoviev, *Codes, Bent Functions and Permutations Suitable for DES-Like Cryptosystems*, Designs, Codes and Cryptography, Vol. 15, No. 2, (1998) 125–156.

[7] C. Carlet, C. Ding, J. Yuan, *Linear Codes From Perfect Nonlinear Mappings and Their Secret Sharing Schemes*, IEEE Trans. Inform. Th., Vol. 51, **6**, (2005) 2089–2013

[8] I. Constantinescu and W. Heise, *A Metric for Codes over Residue Class Rings of Integers*, Problemy Peredachi Informatsii, 33 (3) (1997).

[9] P. Delsarte, *Weights of linear codes and strongly regular normed spaces*, Discrete Math., **3** (1972) 47–64.

[10] M. Greferath and S. E. Schmidt, *Finite-Ring Combinatorics and MacWilliams Equivalence Theorem*, J. of Combinatorial Theory (A) **92** (2000), 17–28.

[11] M. Greferath, A. Nechaev, R. Wisbauer, *Finite Quasi-Frobenius Modules and Linear Codes*, Journal of Algebra and its Application, **3** (3) (2004) 247–272.

[12] M. Greferath and M. E. O'Sullivan, *On Bounds for Codes over Frobenius Rings under Homogeneous Weights*, Discrete Mathematics **289** (2004), 11–24.

[13] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[14] R. C. Heimiller, *Phase Shift Pulse Codes with Good Periodic Correlation Properties*, IRE Transactions on Information Theory, IT-7 (1961) 254–257.

[15] T. Honold, *A Characterization of Finite Frobenius Rings*, Arch. Math. (Basel), **76** (2001).

[16] T. Honold, *Further Results on Homogeneous Two-Weight Codes*, Proceedings of Optimal Codes and Related Topics, Bulgaria (2007).

[17] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, 1999.

[18] B. R. McDonald, *Finite Rings With Identity*, Pure and Applied Mathematics, M. Dekker, New York (1974).

[19] R. Raghavendran, *Finite Associative Rings*, Compositio Math., 21 (1969) 195-229.

[20] J. Yuan, C. Carlet, C. Ding, *The Weight Distribution of a Class of Linear Codes From Perfect Nonlinear Functions*, IEEE Trans. Inform. Th., Vol. 52, **2** (2006) 712–717.